

Herstellereklärung

Der Hersteller

bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG

Am Fallturm 9

D-28359 Bremen

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹

in Verbindung mit § 15 Abs. 5 SigV²,

dass sein Produkt

Governikus, Version 3.2.1.0 (OSCI)

die nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung in Teilen erfüllt.

Bremen, den 04.12.2008

Dr. Stephan Klein

Geschäftsführung

Diese Herstellereklärung mit der Dokumentennummer bos2008004 besteht aus 18 Seiten.

¹ Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05. Mai 2001 (BGBl. I S. 876)), zuletzt geändert durch Artikel 4 des Gesetzes vom 04.01.200526. Februar 2007 (BGBl. I S. 2)179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11. November 2001 (BGBl. I S. 3074)), zuletzt geändert durch 1. SigÄndG Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Dokumentenhistorie

Version	Datum	Bemerkung
1.0	21.05.2008	Initialversion
1.1	29.10.2008	Gesamtüberarbeitung
1.2	25.11.2008	Überarbeitung aufgrund von Rückfragen
1.3	04.12.2008	Überarbeitung (Abschnitt 5.2 und 5.4) aufgrund von Rückfragen

Beschreibung des Produkts

1. Handelsbezeichnung

Die Handelsbezeichnung lautet: Governikus, Version 3.2.1.0 (OSCI)³

Auslieferung: online per Download

Hersteller: bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG

Handelsregisterauszug: HRA 22041

2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktbestandteile	Bezeichnung	Version	Übergabeform
Software	Governikus, Version 3.2.1.0 (OSCI) mit den Teilkomponenten OSCI-Client-Enabler, OSCI-Manager und OSCI-Backend-Enabler	3.2.1.0	online per Download
Handbuch	Betriebshandbuch „Governikus – Teil der virtuellen Poststelle des Bundes“	3.2.1.0	online per Download
	Entwicklerhandbuch „Governikus – Teil der virtuellen Poststelle des Bundes“	3.2.1.0	online per Download
	Installation „Governikus – Teil der virtuellen Poststelle des Bundes“	3.2.1.0	online per Download

Tabelle 1: Lieferumfang und Versionsinformation

Die Software „Governikus, Version 3.2.1.0 (OSCI)“ besteht aus den in der folgenden Tabelle aufgeführten Dateien:

Bibliothek	Beschreibung	Version
commons-logging.jar	Apache Group Commons-Logging	1.0.3
BC134withExtensions_signed.jar	BOS - Bouncycastle	1.3.4
osci-bibliothek.jar	OSCI-Bibliothek	1.2.3
certificatechooser.jar	Auswahl von SmartCard-Zertifikaten über OCF-Keystore	-
CertificateViewer.jar	Ansicht für X509-Zertifikate	-
streamedpkcs7.jar	Laden großer PKCS#7-Dateien	-

³ Dieses Produkt stellt die Weiterentwicklung eines gemäß Common Criteria evaluierten und zertifizierten sowie gemäß Signaturgesetz bestätigten Produktes dar: Virtuelle Poststelle des Bundes (OSCI), Version 2.2.2.6 (vgl. Zertifizierungs-ID: BSI-DSZ-CC-0330-2007; Bestätigungs-ID: BSI.02069.TE.11.2007) sowie Version 2.2.3.2. (vgl. Zertifizierungs-ID: BSI-DSZ-CC-0505; Bestätigungs-ID: BSI.02099.TE.xx.200x).

Bibliothek	Beschreibung	Version
commons-httpclient-3.0.1.jar	Transport	3.0.1
mail.jar	Abbildung von SMIME-Objekten	1.3.1
xmlsec-1.4.1.jar	Abbildung von XML-Signature	1.4.1
activation.jar	JavaBeans Activation Framework	1.0.2
jRegistryKey.jar	Auslesen der Windows-Registry	1.2.3
log4j-1.2.8.jar	Apache Group Log4j-Logging	1.2.8
hsqldb.jar	HSQL Datenbank Treiber (optional)	1.7.1.a
itext-1.4.5.jar	Erstellung von pdf-Dateien (benötigt vom Verificationclient)	1.4.5
jai_codec.jar	Java Advanced Imaging Codecs (benötigt von der Visualisierung)	1.1.2
jai_core.jar	Grafikbibliothek zur Bildanzeige (benötigt von der Visualisierung)	1.1.2
jhall.jar	Java Help (benötigt von der Visualisierung)	2.0_01
Gov2OsciServer.ear	Ear mit dem OSCI Manager und dem Backend-enabler	3.2.1.0
Gov2OsciManager.ear	Ear mit dem OSCI Manager	3.2.1.0
Gov2OsciBackendEnabler.ear	Ear mit dem Backend Enabler	3.2.1.0
Gov2OsciServer_test.ear	Ear mit dem OSCI Manager und dem Backend Enabler sowie den zugehörigen Tests	3.2.1.0
Gov2OsciManager_test.ear	Ear mit dem OSCI Manager sowie den zugehörigen Tests	3.2.10
Gov2OsciBackendEnabler_test.ear	Ear mit dem Backend Enabler sowie den zugehörigen Tests	3.2.1.0
BusinessConnectorExt.jar CertificateViewer.jar clientenabler.jar govBackend_Connectors_Common.jar osci-bibliothek_server.jar	Bibliotheken, die vom OSCI Manager und vom Backend Enabler benötigt werden	3.2.1.0
govOsciBackend_con_impl_ext.rar	Standard Connector, wird vom OSCI Manager und vom Backend Enabler benötigt	3.2.1.0

Tabelle 2: Auflistung der Dateien

Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ nutzt die folgenden nach SigG bestätigten Produkte, die von Dritten hergestellt werden und nicht Bestandteil dieser Erklärung sind (z.B. Kartenleser oder sichere Signaturerstellungseinheit (SSEE)):

Produktklasse	Bezeichnung	Beschreibung + Registriernummer der Bestätigung
SSEE	Produktzentrum Tele-Sec der Deutschen Telekom AG	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0
SSEE	Bundesnotar-kammer,	Signaturerstellungseinheit
		TUVIT.09361.TE.10.2001 Nachtrag vom 24.03.2004
		TUVIT.93100.TE.09.2005

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
	Zertifizierungsstelle	einheit STARCOS 3.0	
SSEE	DATEV eG Zertifizierungsstelle	Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005
SSEE	D-Trust GmbH	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005
SSEE	TC TrustCenter TrustCenter GmbH	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	D-Trust GmbH	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA-Signaturkarte, Version 5.02 der Gemplusmids GmbH	TUVIT.09385.TU.09.2004
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.09395.TU.01.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.09397.TU.03.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.93125.TU.12.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.4 der Giesecke & Devrient GmbH	TUVIT.93123.TU.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA-Signaturkarte, Version 5.10 der Gemplus-	TUVIT.93132.TU.06.2006

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		mids GmbH	
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH	TUVIT.93129.TU.03.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3 der Sagem Orga GmbH	BSI.02076.TE.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	ZKA-Signaturkarte, Version 5.11 Gemplus GmbH (Gematlo)	TUVIT.93138.TU.11.2006
SSEE	Deutsche Rentenversicherung Bund	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
Kartenleser	Utimaco SW AG	Chipkartenlesegerät CardMan®	debisZERT.02013.TE.05.1998
Kartenleser	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	Cherry GmbH	Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12.2004
Kartenleser	Cherry GmbH	PC-Tastaturen mit Chipkartenterminal G83-6700LPZxx/00, G83-6700LQZxx/00	TUVIT.09327.TE.10.2001
Kartenleser	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.08	BSI.02059.TE.02.2006
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack e-com, Version 2.0	T-Systems. 09363.TE.06.2002
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack pinpad, Version 2.0	T-Systems. 09362.TE.05.2002
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser, cyberJack pinpad, Versi-	TUVIT.93107.TU.11.2004

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		on 3.0	
Kartenleser	Kobil Systems GmbH	Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3	BSI.02050.TE.12.2006
Kartenleser	Kobil Systems GmbH	KOBIL Chipkartenterminal KAAN Professional HW-Version KCT100, FW 2.08 GK 1.04	TUVIT.09331.TE.03.2002
Kartenleser	Kobil Systems GmbH	KOBIL Klasse 2 Chipkartenterminals KAAN Standard Plus, FW-Version 02121852	TUVIT.09354.TE.05.2003
Kartenleser	SCM Microsystems GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03.2003

Tabelle 3: Zusätzliche, nach SiG bestätigte Produkte

Zur Unterstützung der Prüffunktionalität, nutzt das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ außerdem die folgenden zu Signaturgesetz und -verordnung konformen Produkte, die ebenfalls von der bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG hergestellt werden, jedoch nicht Bestandteil dieser Erklärung sind:

Produktklasse	Hersteller	Bezeichnung
Signaturanwendungs-komponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Virtuelle Poststelle des Bundes (Basis), Version 2.2.2.6 ⁴

Signaturanwendungs-komponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Governikus, Version 3.2.1.0 (Basis) ⁵
-------------------------------	--	--

Tabelle 4: Zusätzliche SigG- und SigV-konforme Produkte

⁴ Die Software „Virtuelle Poststelle des Bundes (Basis) Version 2.2.2.6“ ist als Signaturanwendungs-komponente unter der Registriernummer BSI.02070.TE.11.2007 nach SigG bestätigt.

⁵ Zur Software „Governikus, Version 3.2.1.0 (Basis)“ ist gemäß § 17 Abs. 4 Satz 2 SigG unter der Dokumentennummer bos2008003 bei der Bundesnetzagentur eine Herstellereklärung hinterlegt.

3. Funktionsbeschreibung

Die Software „Governikus, Version 3.2.1.0 (OSCI)“ ist als Teil einer Signaturanwendungskomponente eine Funktionsbibliothek⁶ – d. h. keine vollständige Signaturanwendungskomponente – und stellt damit eine Basis für weitere Signaturanwendungskomponenten dar.

Das Online Services Computer Interface (OSCI)-Protokoll stellt einen Standard im E-Government dar, in dem zwei Kommunikationspartner (OSCI-Client oder -Backend) über einen OSCI-Intermediär kommunizieren (vgl. www.osci.de).

Der EVG besteht aus den folgenden Teilsystemen:

- OSCI-Client-Enabler;
- OSCI-Manager;
- OSCI-Backend-Enabler.

Der OSCI-Client-Enabler wird auf einem Rechner in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]⁷ mit einem OSCI-Client betrieben, der von einem Benutzer beispielsweise über eine GUI benutzt wird. Der OSCI-Client-Enabler verfügt über die Einbindung von Chipkartenlesern. Der OSCI-Client ist nicht Bestandteil der Software „Governikus, Version 3.2.1.0 (OSCI)“.

OSCI-Manager und -Backend-Enabler werden auf Servern in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]⁷ betrieben, mit jeweiligen Web-Oberflächen (GUIs) von Administratoren konfiguriert und arbeiten im Produktivbetrieb automatisiert und ohne menschliche Aktivitäten. Der OSCI-Backend-Enabler wird von einem OSCI-Backend genutzt. Das OSCI-Backend ist nicht Bestandteil der Software „Governikus, Version 3.2.1.0 (OSCI)“.

Die Software „Governikus, Version 3.2.1.0 (OSCI)“ stellt folgende Funktionalitäten zur Verfügung:

OSCI-Client-Enabler:

- Der OSCI-Client-Enabler unterstützt den Signaturschlüssel-Inhaber bei der Erzeugung von qualifizierten elektronischen Signaturen, die lokal von einer sicheren Signaturerstellungseinheit erzeugt werden.

Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine sichere Signaturerstellungseinheit (SSEE) und den Chipkartenleser.

Es findet kein automatisierter Prozess statt, der nach Eingabe der PIN diese für das System vorhält, zum Signieren automatisch abrufen und an die SSEE sendet.

⁶ Diese Funktionsbibliothek wird für OSCI-Clients bzw. -Backends verwendet, die ihrerseits den OSCI-Client-Enabler resp. -Backend-Enabler aufrufen. Der OSCI-Backend-Enabler verfügt beispielsweise über keine Anzeige.

⁷ Quelle: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19. Juli 2005.

Zur Erzeugung qualifizierten elektronischen Signaturen nutzt der OSCI-Client-Enabler eigene lokale Funktionen; eine Basiskomponente wird hierzu explizit nicht verwendet. Erzeugt werden lediglich Einzelsignaturen.

- Der OSCI-Client-Enabler erhält von einem OSCI-Client die Anforderung⁸, die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen. Der OSCI-Client-Enabler führt eine Signaturprüfung durch, d. h. prüft die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren und visualisiert das Verifikationsergebnis (gültige oder ungültige Signatur oder Fehlermeldung).
- Der OSCI-Client-Enabler erhält von einem OSCI-Client die Anforderung, eine Statusprüfung eines qualifizierten Zertifikats durchzuführen. Während die eigentliche Statusprüfung gemäß OSCI-Protokoll vom OSCI-Intermediär durchgeführt wird, führt der OSCI-Client-Enabler eine Plausibilitätsprüfung durch, in der der OSCI-Client-Enabler prüft, ob das im Laufzettel enthaltene Ergebnis der Zertifikats-Statusprüfung zum Zertifikat der OSCI-Nachricht passt, prüft die elektronische Signatur des Laufzettels und visualisiert das Validierungsergebnis.
- Insgesamt prüft der OSCI-Client-Enabler lokal
 - die mathematische Korrektheit der qualifizierten elektronischen Signatur des Absenders sowie
 - die elektronische Signatur des Laufzettels des OSCI-Managers, auf dem u.a. das Ergebnis der Validierung dokumentiert ist, die der OSCI-Manager durchgeführt hat und die die folgenden Prüfungen umfasst:
 - Ist das Herausgeberzertifikat gültig (d.h. bekannt und nicht gesperrt)?
 - Hat die unterzeichnende Person innerhalb des Gültigkeitszeitraumes ihres qualifizierten Zertifikats signiert (Kettenmodell)?
 - Ist dem Zertifizierungsdiensteanbieter (ZDA) das verwendete qualifizierte Zertifikat bekannt und ist es nicht gesperrt?

Der OSCI-Client-Enabler führt keine eigene Zertifikatsprüfung durch.

- Der OSCI-Client-Enabler bietet eine sichere Anzeige von folgenden zu signierenden und signierten Daten: plain-text (UTF-8-codiert) und tiff-Daten.

Darüber hinaus bietet der OSCI-Client-Enabler eine sichere Anzeige weiterer signaturrelevanter Informationen;

- Verweis, auf welche Daten sich eine Signatur bezieht;
- der Signatur zugeordnete Signaturschlüssel-Inhaber;
- Inhalte des zugehörigen qualifizierten Zertifikats.

Der OSCI-Client-Enabler bietet des Weiteren hinreichende Anzeigen für folgende Prozesse:

- Signierprozess:

⁸ Die Software „Governikus, Version 3.2.1.0 (OSCI)“ wird unter der Annahme betrieben, dass der OSCI-Client bzw. das OSCI-Backend, welches auf diese Software zugreift, eine Signaturanwendungskomponente gemäß SigG/SigV darstellt.

- Das Erzeugen einer Signatur wird vorher eindeutig angezeigt.
- Das zur Signatur korrespondierende Zertifikat wird angezeigt.
- Das Verifikationsergebnis zum Schutz vor Hashwertmanipulation wird angezeigt.
- Verifikationsprozess: Das Ergebnis der Verifikation wird angezeigt, d. h. es wird angezeigt, ob Daten unverändert sind.
- Validierungsprozess: Das Ergebnis der Validierung wird angezeigt, d. h. es wird angezeigt, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- Dem Nutzer wird das Ergebnis der Prüfung angezeigt:
 - Status o.k.: Alle Prüfungen ergaben "gültig".
 - Status nicht eindeutig: Mindestens eine Prüfung konnte nicht durchgeführt werden.
 - Status nicht o.k.: Mindestens eine Prüfung hatte das Ergebnis "ungültig" zur Folge.

Die Funktionsbibliothek OSCI-Client-Enabler versetzt einen Anwendungsentwickler in die Lage, eigene auf OSCI-Transport basierende Anwendungen in Java zu schreiben. Die vom OSCI-Client-Enabler bereitgestellten Funktionalitäten ermöglichen die effiziente Entwicklung von Programmen, die OSCI-Nachrichten erstellen und verarbeiten können, ohne dass spezielle Kenntnisse der Funktionalität und API der OSCI-Bibliothek nötig sind. Durch die Verwendung des OSCI-Client-Enablers wird die Entwicklungszeit von Anwendungen auf Basis der Konzepte und Vorgaben von OSCI-Transport maßgeblich verkürzt. Darüber hinaus stellt der OSCI-Client-Enabler in Form von Objekten, Konfigurationsdateien und einer API eine komfortable Fassade für die granularen Funktionen der OSCI-Bibliothek zur Verfügung. Die OSCI-Bibliothek ist Bestandteil des OSCI-Client-Enablers.

OSCI-Manager:

- Der OSCI-Manager nimmt die Rolle des OSCI-Intermediärs gemäß OSCI-Transport-Protokoll wahr und stellt die Gültigkeit eines qualifizierten Zertifikats unter Zuhilfenahme einer Basiskomponente⁹ fest.

Die Basiskomponente stellt dabei fest, ob das qualifizierte Zertifikat zum Zeitpunkt des Eingangs beim OSCI-Intermediär vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zu diesem Zeitpunkt bereits begonnen und noch nicht abgelaufen war (Kettenmodell), und übergibt das Ergebnis der Validierung in Form des Verzeichnisdienst-Ergebnisses sowie einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) an den OSCI-Manager.

OSCI-Backend-Enabler:

- Der OSCI-Backend-Enabler erhält von einem OSCI-Backend die Anforderung, die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen. Der OSCI-Backend-Enabler führt eine Signaturprüfung durch, d. h. prüft die mathematische Korrektheit der Signatur

⁹ Produkte „Governikus (Basis)“ oder „Virtuelle Postelle des Bundes (Basis)“

mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren und liefert das Ergebnis (gültige oder ungültige Signatur oder Fehlermeldung) an das OSCI-Backend zurück.¹⁰

- Der OSCI-Backend-Enabler erhält von einem OSCI-Backend die Anforderung, eine Statusprüfung eines qualifizierten Zertifikats durchzuführen. Während die eigentliche Statusprüfung gemäß OSCI-Protokoll vom OSCI-Intermediär durchgeführt wird, führt der OSCI-Backend-Enabler neben der Prüfung der elektronische Signatur des Laufzettels des OSCI-Managers eine Plausibilitätsprüfung durch, in der der OSCI-Backend-Enabler prüft, ob das im Laufzettel enthaltene Ergebnis der Zertifikats-Statusprüfung zum Zertifikat der OSCI-Nachricht passt, und gibt das Validierungsergebnis (ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren) an das OSCI-Backend zurück.

Die vorliegende Herstellereklärung bezieht sich ausschließlich auf die Eigenschaft der Software „Governikus, Version 3.2.1.0 (OSCI)“ als Signaturanwendungskomponente i. S. d. § 2 Nr. 11 SigG, d.h. auf diejenigen Funktionalitäten, die dazu bestimmt sind,

- Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen und
- qualifizierte Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

Die Software „Governikus, Version 3.2.1.0 (OSCI)“ erfüllt die Anforderungen gemäß § 17 Abs. 2 SigG sowie § 15 Abs. 2 und 4 SigV.

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ erfüllt die nachfolgenden Anforderungen des SigG, wie in der Bestätigungsurkunde zum Vorgängerprodukt „Virtuelle Poststelle des Bundes (OSCI), Version 2.2.2.6 bereits angegeben:

- § 17 Abs. 2 Satz 1 SigG: „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.“
- § 17 Abs. 2 Satz 2 SigG: „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...]
 1. auf welche Daten sich die Signatur bezieht,
 2. ob die signierten Daten unverändert sind,
 3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
 4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und

¹⁰ Die Interaktion mit dem Benutzer erfolgt über das OSCI-Backend, welches nicht Bestandteil der Software „Governikus, Version 3.2.1.0 (OSCI)“ ist.

5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.

- § 17 Abs. 2 Satz 3 SigG: „Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.“

Zur Umsetzung dieser Anforderungen ist in der Software „Governikus, Version 3.2.1.0 (OSCI)“ implementiert:

- eine sichere Anzeige gemäß den Anforderungen des SigG beim OSCI-Client-Enabler:
 - von zu signierenden und signierten Daten in Format plain-text (UTF-8-codiert) und tiff;
 - weiterer signatur-relevanter Informationen;
 - Verweis, auf welche Daten sich eine Signatur bezieht;
 - der Signatur zugeordnete Signaturschlüssel-Inhaber;
 - Inhalte des zugehörigen qualifizierten Zertifikats;
 - zum Signierprozess:
 - das Erzeugen einer Signatur wird vorher eindeutig angezeigt;
 - das zur Signatur korrespondierende Zertifikat wird angezeigt;
 - das Verifikationsergebnis zum Schutz vor Hashwertmanipulation wird angezeigt;
 - zum Verifikationsprozess: Das Ergebnis der Verifikation wird angezeigt, d. h. es wird angezeigt, ob Daten unverändert sind.
 - zum Validierungsprozess: Das Ergebnis der Validierung wird angezeigt, d. h. es wird angezeigt, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- Verifikation von Signaturen (lokale mathematische Prüfung) beim OSCI-Client-Enabler und OSCI-Backend-Enabler.

Hinweis: Die eigentliche Validierung von Zertifikaten (Überprüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren) erfolgt unter Zuhilfenahme einer Basiskomponente, mit der der OSCI-Manager die Rolle des OSCI-Intermediärs wahrnimmt.

Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ erfüllt die nachfolgenden Anforderungen der SigV:

- § 15 Abs. 2 Nr. 1c) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur [...] c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird [...]“. Nur der OSCI-Client-Enabler unterstützt diese Anforderung durch entsprechende Anzeigen.
- § 15 Abs. 2, Nr. 2a) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] 2. bei der Prüfung einer qualifizierten elektronischen Signatur a) die Korrektheit der Signatur zuverlässig geprüft und angezeigt wird“. Sowohl OSCI-Client-Enabler als auch der -Backend-Enabler stellen diese Funktionalität den sie integrierenden Fachverfahren zur Verfügung. Die Anzeige erfolgt nur beim OSCI-Client-Enabler.

- § 15 Abs. 2, Nr. 2b) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] 2. bei der Prüfung einer qualifizierten elektronischen Signatur b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren“. Sowohl OSCI-Client-Enabler als auch der -Backend-Enabler stellen diese Funktionalität den sie integrierenden Fachverfahren zur Verfügung. Die Anzeige erfolgt nur beim OSCI-Client-Enabler.
- § 15 Abs. 4 SigV: „Sicherheitstechnische Veränderungen an technischen Komponenten [...] müssen für den Nutzer erkennbar sein“. Das Prüftool¹¹ erlaubt nur eine Integritätsprüfung des OSCI-Client-Enablers. Die Integrität des OSCI-Managers und des OSCI-Backend-Enablers muss durch die Einsatzumgebung sichergestellt werden. Siehe dazu die Anforderungen an den Betrieb der Server.

Hinweis: Die eigentliche Validierung von Zertifikaten (Überprüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren) erfolgt unter Zuhilfenahme einer Basiskomponente.

Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ erfüllt die folgenden Anforderungen explizit **nicht**:

- § 15 Abs. 2 Nr. 1a) und b) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
 - b) eine Signatur nur durch die berechtigt signierende Person erfolgt [...]“.Diese Anforderungen werden durch sichere Signaturerstellungseinheiten (Signaturkarten) und Chipkartenleser realisiert (vgl. Auflistung in Abschnitt 2).
- Des Weiteren ist für den OSCI-Backend-Enabler – im Gegensatz zum OSCI-Client-Enabler – keine sichere Anzeige enthalten, so dass die gesetzlichen Anforderungen nicht erfüllt werden. Darüber hinaus obliegt dem OSCI-Backend, der auf den OSCI-Backend-Enabler zugreift, insbesondere festzustellen, „welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist“ und „welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen“ (§ 17 Abs. 2 Satz 2 Nr. 3 und 4 SigG).

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software „Governikus, Version 3.2.1.0 (OSCI)“ wird folgende Einsatzumgebung vorausgesetzt:

serverseitig:

- AMD/Intel-PC mit 2 GB Hauptspeicher (RAM);

¹¹ Das Prüftool ist nicht Bestandteil der Auslieferung und wird auf Wunsch vom Hersteller zur Verfügung gestellt.

- Betriebssystem:
 - Microsoft Windows 2003 Server;
 - SUSE Linux Enterprise Server 10;
 - RedHat Enterprise 5
 - Solaris 9;
 - Solaris 10;
 - HP UX 11.11.
- Basiskomponente gemäß Tabelle 4

clientseitig:

- AMD/Intel-PC mit
 - 512 MB Hauptspeicher (RAM) und
 - 100 MB Plattenplatz;
- Betriebssystem:
 - Microsoft Windows 2000, XP, Vista (jeweils mit aktuellem Service Pack);
 - openSuSE 10.x;

sowohl client- als auch serverseitig:

- Signaturkarte gemäß Tabelle 3, wobei die Auflagen aus der Bestätigung zu dem Produkt (siehe Registriernummer in Tabelle 3) einzuhalten sind;
- Chipkarten-Lesegerät gemäß Tabelle 3, wobei die Auflagen aus der Bestätigung zu dem Produkt (siehe Registriernummer in Tabelle 3) einzuhalten sind;
- Java Runtime Environment (JRE), Version 1.5.0 und Version 1.6.
- OSCI-Client und OSCI-Backend, die von außen über eine Schnittstelle auf den EVG zugreifen und Funktionalitäten des Produktes nutzen, stehen zur Verfügung und erfüllen die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente.

Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

5.2 Anbindung an ein Netzwerk

Zur Anbindung des Produktes „Governikus, Version 3.2.1.0 (OSCI)“ an ein Netzwerk müssen die folgenden Maßnahmen zum Schutz beachtet werden: Netzwerkverbindungen müssen so abgesichert sein, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, geeignete Absicherung des LAN und durch die Verwendung geeigneter Anti-Viren-Programme.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

Die Auslieferung erfolgt online per Download von einem Webserver.¹²

Alle Dateien der Software „Governikus, Version 3.2.1.0 (OSCI)“ werden vor der Auslieferung vom Hersteller signiert, um Schutz vor unerkannten nachträglichen Manipulationen und Veränderungen zu bieten. Der Nutzer sollte sich vor der Installation der Software „Governikus, Version 3.2.1.0 (OSCI)“ von der Gültigkeit der Signatur überzeugen. Die Verifikation der Signatur erfolgt über Standard-Java-Mechanismen.

Zudem ist die Integrität und Authentizität des OSCI-Client-Enablers mit dem vom Hersteller zur Verfügung gestellten Prüftool zu prüfen.

Die Installation des „Governikus, Version 3.2.1.0 (OSCI)“ wird ausführlich im Handbuch erläutert.

5.4 Auflagen für den Betrieb des Produktes

Während des Betriebs sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

Auflagen zur Sicherheit der IT-Plattform und Applikationen

Es muss gewährleistet sein, dass von der Hardware, auf der die Software „Governikus, Version 3.2.1.0 (OSCI)“ betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass

- die auf dem eingesetzten Personalcomputer installierte Software – insbesondere die Java Virtual Maschine – nicht böswillig manipuliert oder verändert werden kann,
- auf dem Personalcomputer keine Viren oder Trojanischen Pferde eingespielt werden können,
- die Hardware des Personalcomputers nicht unzulässig verändert werden kann,
- der verwendete Chipkartenleser nicht böswillig manipuliert wurde, um Daten (z. B. PIN, Hashwerte etc.) auszuforschen oder zu verändern.

Das Ausforschen der PIN auf dem Personalcomputer kann nur dann mit Sicherheit ausgeschlossen werden, wenn ein Chipkartenleser mit sicherer PIN-Eingabe eingesetzt wird.

Rechner und Chipkartenleser sind durch einen sicheren Kanal per Kabel verbunden.

Zudem ist für den OSCI-Client-Enabler ein Prüftool zum Schutz vor unbefugter Veränderung (Integritätsschutz) verfügbar.

Für die serverseitigen Komponenten (OSCI-Manager und -Backend-Enabler) muss darüber hinaus gewährleistet sein:

- Für den Betrieb ist vertrauenswürdigen Personal eingesetzt, das einen Beitrag zur Sicherheit leistet, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb der serverseitigen Komponenten des EVG (OSCI-Manager und -Backend-Enabler) sind vorhanden.

¹² Abweichend von der bestätigten Vorgängerversion dieses Produktes wird für diese Version ausschließlich die Online-Auslieferung via Download angeboten.

- Es sind verschiedene Administratoren für die verschiedenen Aufgaben benannt, die einen Beitrag zur Sicherstellung einer vertraulichen und integren Betriebsumgebung des EVG leisten. Ein Vier-Augen-Prinzip mit Revisor ist für wichtige Aktivitäten organisatorisch realisiert.
- Es wird gewährleistet, dass der EVG korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzelnen Systemkomponenten mit Firewall, Demilitarisierter Zone (DMZ) etc. OSCI-Manager und Kernsystem der Basiskomponente werden zusammen innerhalb eines vertrauenswürdigen Netzes betrieben.
- Der OSCI-Backend-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Backend zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute wird vom OSCI-Backend sichergestellt.
- Für die Serverkomponenten sind die folgenden baulichen, personellen und organisatorischen Anforderungen umzusetzen:
 - Rechner, Monitor und Tastatur befinden sich in einem Betriebsraum.
 - Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
 - Wartungs- bzw. Reinigungspersonal erhält den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.

Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Die eingesetzten Systeme müssen gegen einen manuellen Zugriff Unbefugter geschützt werden – insbesondere, um Manipulation von Dateien auf Dateisystemebene, die die Software zur Darstellung der Nachrichten benötigt, zu unterbinden. Dies kann z. B. durch Aufstellung in einem abschließbaren Raum geschehen.

Die Unterrichtung des Zertifizierungsdiensteanbieters zur Handhabung der SSEE ist zu beachten.

Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielen von Daten über Datenträger muss – z. B. durch die Verwendung geeigneter Anti-Viren-Programme – sichergestellt werden, dass keine Viren oder Trojanischen Pferde eingespielt werden können.

Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz der Software „Governikus, Version 3.2.1.0 (OSCI)“ zu beachten:

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Nutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet noch die PIN anderen Personen bekannt gemacht wird.
- Nur bei dem Betrieb eines bestätigten Chipkartenlesers mit PIN-Pad ist sicher gestellt, dass die PIN nur zur SSEE übertragen wird.
- Eine signaturgesetz-konforme Nachprüfung qualifizierter Zertifikate kann nur erfolgen, soweit dafür die technischen Voraussetzungen – etwa durch eine Verbindung zu einer Basiskomponente – gegeben sind.

Auflagen für Wartung/Reparatur

Eine Pflege und Wartung der Software „Governikus, Version 3.2.1.0 (OSCI)“ ist nicht vorgesehen. Ggf. erfolgt eine Aktualisierung über einen Download von einem Webserver.

6. Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt Governikus, Version 3.2.1.0 (OSCI) die Hashfunktionen SHA-256 und RIPEMD-160 bereitgestellt.¹³

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt Governikus, Version 3.2.1.0 (OSCI) die Hashfunktionen SHA-256, RIPEMD-160 und SHA-1 sowie der Signaturalgorithmus RSA bereitgestellt.

Die gemäß Abs. 1 Nr. 2 SigV festgelegte Eignung für die verwendeten kryptographischen Algorithmen SHA-256, RIPEMD-160 und SHA-1 sind gemäß den Angaben der Bundesnetzagentur (vgl. „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn vom 17. Dezember 2007, veröffentlicht am 05. Februar 2008 im Bundesanzeiger Nr. 19, S. 376) wie folgt als geeignet eingestuft:

- RIPEMD-160: gültig bis 31.12.2010;
- SHA-2 Familie (SHA-224, SHA-256, SHA-384, SHA-512): gültig bis 31.12.2014;
- SHA-1: ungültig; war gültig bis 30.6.2008 (Der Benutzer kann über OSCI-Client resp. -Backend die Prüfung eines Zertifikates zu einem zurückliegenden Prüfzeitpunkt anfordern, zu dem SHA-1 noch gültig gewesen sein kann.)
- RSA mit Schlüssellänge 2048 Bit: gültig bis 31.12.2014.

7. Gültigkeit der Herstellereklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2010 gültig. Die Gültigkeit der Herstellereklärung ist weiter beschränkt durch die in Kapitel 6 aufgeführten Gültigkeiten der Algorithmen; die Gültigkeit kann sich verkürzen, wenn z.B. neue Feststellungen hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Qualifizierte Elektronische Signatur – Technischer Betrieb) zu erfragen.

8. Zusatzdokumentation

Folgende Bestandteile der Herstellereklärung wurden aus dem Veröffentlichungstext ausgegliedert und bei der zuständigen Behörde hinterlegt:

¹³ Hinweis: Das Produkt „Governikus, Version 3.2.1.0 (OSCI)“ unterstützt ferner die Hashfunktion SHA-1, die allerdings zum 30.6.2008 ausgelaufen ist, so dass aufgrund der abgelaufenen oder gesperrten Zertifikate keine qualifizierten elektronischen Signaturen mehr erzeugt werden können.

- „Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software ‚Governikus, Version 3.2.1.0 (OSCI)‘ – Sicherheitstechnische Produktbeschreibung, Spezifikation und Tests“, 21.05.2008, 15 Seiten.
- „Betriebshandbuch ‚Governikus – Teil der virtuellen Poststelle des Bundes,“, Dokument-Version 3.2.1.0_0, 10.04.2008, 217 Seiten.
- „Entwicklerhandbuch ‚Governikus – Teil der virtuellen Poststelle des Bundes“, Dokument-Version 3.2.1.0_0, 10.04.2008, 70 Seiten.
- „Installation ‚Governikus – Teil der virtuellen Poststelle des Bundes“, Dokument-Version 3.2.1.0_0, 10.04.2008, 103 Seiten.
- Testhandbuch „OSCI-Komponenten“, Dokument-Version 0.7, 17.08.2007, 44 Seiten
- Testdokumentation Governikus_3210_OSCIServer_BackEnd_Testprotokoll.xls
- Testdokumentation OSCI_ClientEnabler_Testprotokoll_WINXP.xls
- Testdokumentation OSCI_ClientEnabler_Testprotokoll_LINUX.xls
- Testdokumentation Produktivtest_Kartenansteuerung_XP.xls
- Testdokumentation Produktivtest_Kartenansteuerung_2000.xls
- Testdokumentation Produktivtest_Kartenansteuerung_Vista64Bit.xls
- „Sicherheitsvorgaben (ST), Virtuelle Poststelle des Bundes 2.2.x.x (OSCI)“, Dokument-Version 0.4, 19.07.2006, 97 Seiten
- „Funktionale Spezifikation (ADV_FSP) ‚Virtuelle Poststelle des Bundes 2.2.x.x (OSCI)“, Dokument-Version 0.92, 01.02.2007, 69 Seiten
- „Virtuelle Poststelle des Bundes 2.2.x.x (Re-Evaluierung) Änderungsdocument zu Funktionale Spezifikation (ADV_FSP), Dokument-Version 0.3, 15.10.2007, 13 Seiten
- Virtuelle Poststelle des Bundes 2.2.x.x (OSCI) Entwurf auf hoher Ebene (ADV_HLD), Dokument-Version 0.93, 06.09.2007, 64 Seiten
- Virtuelle Poststelle des Bundes 2.2.3.x, Änderungen zum Dokument Entwurf auf hoher Ebene (ADV_HLD), Dokument-Version 0.21, 22.10.2007, 21 Seiten

Ende der Herstellereklärung